スマートカードおよび証明書によるログインのサポート

OnCommand Insight

NetApp
April 01, 2024

目次

スマートカードおよび証明書によるログインのサポート

OnCommand Insight では、Insightサーバにログインするユーザの認証にスマートカード（CAC）と証明書を使用できます。これらの機能を有効にするには、システムを設定する必要があります。

CACと証明書をサポートするようにシステムを設定した後、OnCommand Insight の新しいセッションに移動すると、ブラウザにネイティブダイアログが表示され、選択する個人証明書のリストが表示されます。これらの証明書は、OnCommand Insight サーバによって信頼されたCAによって発行された個人証明書のセットに基づいてフィルタリングされます。ほとんどの場合、単一の選択があります。既定では、選択肢が1つしかない場合、Internet Explorerはこのダイアログをスキップします。

CACユーザの場合、スマートカードには複数の証明書が含まれており、信頼されたCAに一致できる証明書は1つだけです。のCAC証明書 `identification` を使用する必要があります。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされている OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

スマートカードおよび証明書によるログイン用にホストを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight ホストの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザのIDを含むLDAPフィールドと一致する必要があります。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされている OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. を使用します `regedit` でレジストリ値を変更するユーティリティ `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`：
   a. jvm_optionを変更します `DclientAuth=false` 終了： `DclientAuth=true.`
2. キーストアファイルをバックアップします。 `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. コマンドプロンプトを開き、を指定します `Run as administrator`
4. 自己生成証明書を削除します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 新しい証明書を生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. 証明書署名要求（CSR）を生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. 手順6でCSRが返されたら、証明書をインポートし、Base-64形式でエクスポートしてに保存します `"C:\temp" named servername.cer`。
8. キーストアから証明書を抽出します。`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. p12ファイルから秘密鍵を抽出します。 `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`

10. 手順7でエクスポートしたBase-64証明書を秘密鍵とマージします。 `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. マージした証明書をキーストアにインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. ルート証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. ルート証明書をserver.trustoreにインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. 中間証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    すべての中間証明書について、この手順を繰り返します。

15. この例と一致するようにLDAPでドメインを指定します。
16. サーバを再起動します。

スマートカードおよび証明書によるログインをサポートするようにクライアントを設定しています

クライアントマシンでスマートカードを使用し、証明書によるログインを有効にするには、ミドルウェアを使用し、ブラウザを変更する必要があります。スマート・カードをすでに使用しているお客様は、クライアント・マシンに追加の変更を加える必要はありません。

作業を開始する前に

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされている OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

一般的なクライアント設定要件は次のとおりです。

- ActivClientなどのスマートカードミドルウェアのインストール（を参照）
- IEブラウザの変更（を参照
- Firefoxブラウザの変更（を参照

Linuxサーバでの**CAC**の有効化

Linux OnCommand Insight サーバでCACを有効にするには、いくつかの変更が必要です。

手順

1. に移動します `/opt/netapp/oci/conf/`
2. 編集 `wildfly.properties` をクリックし、の値を変更します `CLIENT_AUTH_ENABLED` 「True」へ
3. にある「ルート証明書」をインポートします `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. サーバを再起動します

Data Warehouseでスマートカードおよび証明書によるログインを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight データウェアハウスの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザの政府機関ID番号を含むLDAPフィールドと一致する必要があります。

  政府発行のCACに保存される共通名（CN）は、通常次の形式になります。 `first.last.ID`。一部のLDAPフィールド（など）`sAMAccountName`この形式は長すぎます。これらのフィールドの場合、OnCommand Insight はCNからID番号だけを抽出します。

> CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。
>
> - "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
> - "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
> - "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
> - "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
> - "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. regeditを使用して、のレジストリ値を変更します `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. jvm_optionを変更します `-DclientAuth=false` 終了： `-DclientAuth=true`。

   Linuxの場合は、を変更します `clientAuth` のパラメータ `/opt/netapp/oci/scripts/wildfly.server`

2. Data Warehouse TrustoreにCertificate Authority（CA；認証局）を追加します。

   a. コマンドウィンドウで、に進みます `..\SANscreen\wildfly\standalone\configuration`。

   b. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      各行の最初の単語はCAエイリアスを示します。

   c. 必要に応じて、CA証明書ファイル（通常は）を指定します `.pem` ファイル。Data Warehouseの信頼済みCAにお客様のCAを含めるには、に進みます `..\SANscreen\wildfly\standalone\configuration` およびを使用します `keytool` インポートコマンド： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v`

`-trustcacerts`

my_aliasは通常、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。

3. OnCommand Insight サーバで、を実行します `wildfly/standalone/configuration/standalone-full.xml` でverify-clientを「requested」に更新して、ファイルを変更する必要があります `/subsystem=undertow/server=default-server/https-listener=default-https`CACを有効にします。Insight Serverにログインし、該当するコマンドを実行します。

OS	スクリプト
Windows の場合	<install dir> を参照してください\enableCACforRemoteEJB.bat
Linux の場合	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

スクリプトの実行後、wildflyサーバのリロードが完了するまで待ってから、次の手順に進みます。

4. OnCommand Insight サーバを再起動します。

スマートカードおよび証明書によるログインのためのCognosの設定（OnCommand Insight 7.3.5~7.3.9）

Cognosサーバでスマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight Data Warehouseの設定を変更する必要があります。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.5~7.3.9を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. Cognos TrustoreにCertificate Authority（CA；認証局）を追加します。
   a. コマンドウィンドウで、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`
   b. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ：
      ```
      ..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet
      ```
      各行の最初の単語はCAエイリアスを示します。
   c. 適切なファイルが存在しない場合は、CA証明書ファイル（通常は）を指定します `.pem` ファイル。
   d. OnCommand Insight の信頼済みCAに顧客のCAを含めるには、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. を使用します `keytool` をインポートするユーティリティ `.pem` ファイル：
      ```
      ..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts
      ```
      `my_alias` は通常、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。
   f. パスワードの入力を求められたら、と入力します `NoPassWordSet`。
   g. 回答 `yes` 証明書を信頼するように求められたら、
2. CACモードをイネーブルにするには、を実行します `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. CACモードをディセーブルにするには、を実行します `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

スマートカードおよび証明書によるログインのためのCognosの設定（OnCommand Insight 7.3.10以降）

Cognosサーバでスマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight Data Warehouseの設定を変更する必要があります。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされている OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. Cognos TrustoreにCertificate Authority（CA；認証局）を追加します。
   a. コマンドウィンドウで、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`
   b. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      各行の最初の単語はCAエイリアスを示します。
   c. 適切なファイルが存在しない場合は、CA証明書ファイル（通常は）を指定します `.pem` ファイル。
   d. OnCommand Insight の信頼済みCAに顧客のCAを含めるには、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. を使用します `keytool` をインポートするユーティリティ `.pem` ファイル： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` は通常、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。
   f. パスワードの入力を求められたら、と入力します `NoPassWordSet`。
   g. 回答 `yes` 証明書を信頼するように求められたら、
2. CACモードをイネーブルにするには、次の手順を実行します。
   a. 次の手順に従って、CACログアウトページを設定します。
      - Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
      - （7.3.10および7.3.11の場合のみ）[管理]→[構成]→[システム]→[セキュリティ]をクリックします
      - （7.3.10および7.3.11の場合のみ）Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します

- ブラウザを閉じます。

b. 実行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

3. CACモードを無効にするには、次の手順を実行します。

a. 実行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

c. （7.3.10および7.3.11の場合のみ）次の手順に従って、CACログアウトページの設定を解除します。

- Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
- [管理]→[設定]→[システム]→[セキュリティ]をクリックします
- Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します
- ブラウザを閉じます。

CognosおよびDWH用のCA署名SSL証明書のインポート（Insight 7.3.5から7.3.9）

SSL証明書を追加して、Data WarehouseおよびCognos環境の認証と暗号化を強化することができます。

作業を開始する前に

この手順 は、OnCommnand Insight 7.3.5~7.3.9を実行しているシステム用です。

> CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。
>
> - "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
> - "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
> - "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
> - "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
> - "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

この手順 を実行するには、admin権限が必要です。

手順

1. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. の下にある「certs」フォルダと「csk」フォルダのバックアップを作成します `..\SANScreen\cognos\analytics\configuration`。
3. Cognosから証明書暗号化要求を生成します。Admin CMDウィンドウで、次のコマンドを実行します。
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. を開きます `c:\temp\encryptRequest.csr` ファイルを作成し、生成されたコンテンツをコピーします。
5. encryptRequest.csrを認証局（CA）に送信してSSL証明書を取得します。

   「`S an：dns=fqdn」のような属性を追加してください(例: hostname.netapp.com)`"はSubjectAltNameを追加します)。Google Chromeバージョン58以降では、証明書にSubjectAltNameがない場合に苦情が表示されます。

6. PKCS7形式を使用してルート証明書を含め、チェーン証明書をダウンロードします

   FQDNの.p7bファイルがダウンロードされます

7. CAから.p7b形式の証明書を取得します。Cognos Webサーバの証明書としてマークする名前を使用します。
8. ThirdPartyCertificateTool.batはチェーン全体をインポートできないため、すべての証明書をエクスポートするには複数の手順が必要です。チェーンを次のように個別にエクスポートして分割します。
   a. "`Crypto Shell Extensions`"の.p7b証明書を開きます。
   b. 左側のペインで「証明書」を参照します。
   c. ルートCA > All Tasks > Exportを右クリックします。
   d. Base64出力を選択します。
   e. ルート証明書として識別するファイル名を入力します。
   f. 手順8aから8cを繰り返して、すべての証明書を.cerファイルに個別にエクスポートします。
   g. ファイルにmediateX.cerとcognos.cerという名前を付けます。
9. CA証明書が1つしかない場合は、この手順を無視します。それ以外の場合は、root.cerとintermediateX.cerの両方を1つのファイルにマージします。
   a. メモ帳でintermediate.cerを開き、コンテンツをコピーします。
   b. メモ帳でroot.cerを開き、9aの内容を保存します。
   c. ファイルをCA.cerとして保存します。
10. Admin CMDプロンプトを使用して、Cognosキーストアに証明書をインポートします。
    a. cd「Program Files\SANscreen\cognos\analytics\bin`」
    b. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\ca.cer

これにより、CA.cerがルート認証局として設定されます。

c. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\ca.cer

これにより、cognos.cerがca.cerによって署名された暗号化証明書として設定されます。

11. [IBM Cognos Configuration]を開きます。
    a. [Local Configuration]→[Security]→[Cryptography]→[Cognos]を選択します
    b. 「サードパーティCAを使用しますか？」を変更します。 Trueに設定します。
    c. 設定を保存します。
    d. Cognosを再起動します
12. Admin CMDプロンプトを使用して、最新のCognos証明書をcognos.crtにエクスポートします。
    a. "D：\Program Files\SANscreen\Java\bin\keytool .exe"-exportcert -file “c：\temp\cognos.crt”-keystore" D：\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore"-storetype PKCS12 -storepass NoPassWordSet -alias -alias
13. Admin CMDプロンプトウィンドウを使用して、「c：\temp\cognos.crt」をDWH trustoreにインポートし、CognosとDWHの間のSSL通信を確立します。
    a. "D：\Program Files\SANscreen\Java\bin\keytool .exe"-importcert -file “c：\temp\cognos.crt”-keystore" D：\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"-storepass changeit -alias cognoscert
14. SANscreen サービスを再起動します。
15. DWHのバックアップを実行して、DWHがCognosと通信していることを確認します。

CognosおよびDWHのCA署名SSL証明書のインポート（Insight 7.3.10以降）

SSL証明書を追加して、Data WarehouseおよびCognos環境の認証と暗号化を強化することができます。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされている OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

この手順 を実行するには、admin権限が必要です。

手順

1. IBM Cognos Configurationツールを使用してCognosを停止します。Cognosを閉じます。
2. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration` および `..\SANScreen\cognos\analytics\temp\cam\freshness` フォルダ。
3. Cognosから証明書暗号化要求を生成します。Admin CMDウィンドウで、次のコマンドを実行します。
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。注意:ここで-Hと-IはdnsやipaddressのようなsubjectAltNamesを追加します。
4. を開きます `c:\temp\encryptRequest.csr` ファイルを作成し、生成されたコンテンツをコピーします。
5. encryptRequest.csrコンテンツを入力し、CA署名ポータルを使用して証明書を生成します。
6. PKCS7形式を使用してルート証明書を含め、チェーン証明書をダウンロードします

   FQDNの.p7bファイルがダウンロードされます

7. CAから.p7b形式の証明書を取得します。Cognos Webサーバの証明書としてマークする名前を使用します。
8. ThirdPartyCertificateTool.batはチェーン全体をインポートできないため、すべての証明書をエクスポートするには複数の手順が必要です。チェーンを次のように個別にエクスポートして分割します。
   a. "`Crypto Shell Extensions`"の.p7b証明書を開きます。
   b. 左側のペインで「証明書」を参照します。
   c. ルートCA > All Tasks > Exportを右クリックします。

   d. Base64出力を選択します。
   e. ルート証明書として識別するファイル名を入力します。
   f. 手順8aから8eを繰り返して、すべての証明書を.cerファイルに個別にエクスポートします。
   g. ファイルにmediateX.cerとcognos.cerという名前を付けます。
9. CA証明書が1つしかない場合は、この手順を無視します。それ以外の場合は、root.cerとintermediateX.cerの両方を1つのファイルにマージします。
   a. メモ帳でroot.cerを開き、内容をコピーします。
   b. メモ帳を使用してintermediate.cerを開き、9aのコンテンツを追加します（最初に中間、次にルート）。
   c. ファイルをchain.cerとして保存します。
10. Admin CMDプロンプトを使用して、Cognosキーストアに証明書をインポートします。
   a. cd「Program Files\SANscreen\cognos\analytics\bin`」
   b. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\root.cer
   c. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\intermediate.cer
   d. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\chain.cer
11. [IBM Cognos Configuration]を開きます。
   a. [Local Configuration]→[Security]→[Cryptography]→[Cognos]を選択します
   b. 「サードパーティCAを使用しますか？」を変更します。 Trueに設定します。
   c. 設定を保存します。
   d. Cognosを再起動します
12. Admin CMDプロンプトを使用して、最新のCognos証明書をcognos.crtにエクスポートします。
   a. CD "`C：\Program Files\SANscreen"
   b. java\bin\keytool.exe -exportcert -file c：\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias encryption
13. DWHサーバのtrustoreをにバックアップします`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Admin CMDプロンプトウィンドウを使用して、「c：\temp\cognos.crt」をDWH trustoreにインポートし、CognosとDWHの間のSSL通信を確立します。
   a. CD "`C：\Program Files\SANscreen"
   b. java\bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass changeit -alias cognos3rdca
15. SANscreen サービスを再起動します。
16. DWHのバックアップを実行して、DWHがCognosと通信していることを確認します。
17. 次の手順は、「sl certificate」のみを変更し、デフォルトのCognos証明書を変更しない場合でも実行する必要があります。そうしないと、新しいSANscreen 証明書についてCognosから苦情が表示されたり、DWHバックアップを作成できない可能性があります。

a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`

b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass changeit -alias “ssl certificate”`

c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

通常、これらの手順はCognos証明書のインポートプロセスの一環として実行します（を参照） "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"